Internal Audit Manual and RBIA Policy for Vama Sundari Investments (Delhi) Private Limited

DOCUMENT TITLE	INTERNAL AUDIT MANUAL AND RBIA POLICY
DOCUMENT REF NO.	VSIDPL/IA/2025/V2
VERSION NO.	VERSION 2
CHAPTER EFFECTIVE	19th May, 2025
NEXT REVIEW DATE	It is to be reviewed annually

Index

CHAPTER 1: INTRODUCTION

Purpose, Scope and Objective of this Document

The Internal Audit process manual documents the process steps followed by Internal audit in performing various activities viz audit planning, scoping, risk assessment, execution, post audit completion activities. Etc.

The Internal Audit Manual is prepared in accordance with the Audit Committee of Board (ACB) approved internal audit framework.

The objective of this manual is to provide guidance to the Internal audit team and ensure consistency in audit approach and methodology while performing internal audit activities.

The Internal Audit Manual shall be approved by the Head of Internal Audit (HIA),

Any deviation from the Manual shall be as per delegation matrix below:

HIA: Head of Internal Audit

DGM: Deputy General Manager – Internal Audit

CHAPTER 2: ANNUAL AUDIT PLANNING AND RESOURCE BUDGETING

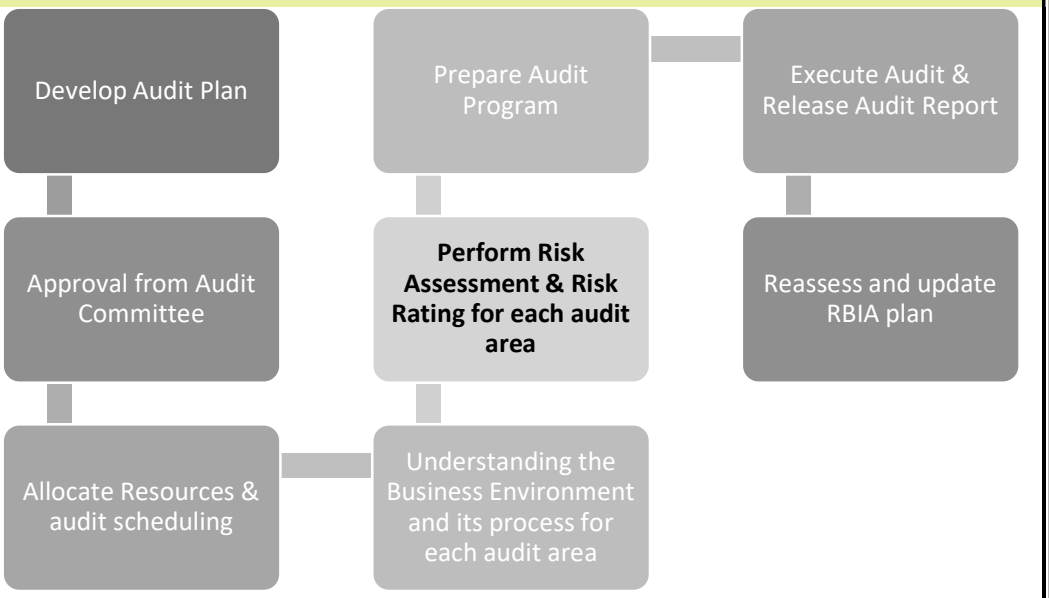
Objectives of Planning

Audit planning is a vital part of the audit, conducted at the beginning of the audit cycle to develop a strategy and a detailed approach for the expected nature, timing and extent of the audit. A well-developed plan helps the Internal Audit function to perform audits in an efficient and timely manner. Internal Audit planning is to be undertaken before the start of the defined audit cycle.

The internal audit plan should be consistent with the goals and objectives of the Internal Audit function and objectives of the organization. Internal audit plan shall be prepared in accordance with the risk based internal audit approach specified by RBI vide circular (Ref. No. DoS.CO.PPG/SEC.05/11.01.005/2020-21) dated 3rd February 2021.

Risk-Based Internal Audit (RBIA) is an audit methodology that links an organization's overall risk management framework and provides an assurance to the Board of Directors and the Senior Management on the quality and effectiveness of the organization's internal controls, risk management and governance related systems and processes.

Risk Based Internal Audit (RBIA) Process:



<table>
<tr><td>Establishing the Audit Universe</td><td>Audit Universe shall include all business products and associated processes by the Company as well as all supporting functions complementing them and ensuring the Audit universe is in line with Operation risk review program. Each unit of the audit universe shall be assigned a risk rating of ‘High’, ‘Medium’, ‘Low’, based on the results of risk assessment.

Following steps are to be followed to define Audit Universe:

i. The Organization chart provided by HR shall be referred for the List of Departments / Functions:
ii. Review the list of functions / departments covered in risk framework
iii. The Departments / Functions shall be sub-divided into major processes / activity and sub-processes.
iv. Group these processes and sub processes into Auditable units
v. Audit Universe and the overall RBIA Plan shall be continuously monitored during the execution phase for achievement of its objective and to identify any deviations.

Completeness of Audit Universe shall be discussed with the respective Leadership team during the annual risk assessment and their inputs taken.

The Audit Universe shall be updated on yearly basis by carrying out the above steps for any additions / deletions of processes / products / functions.</td></tr>
<tr><td>Risk Assessment</td><td>Risk Assessment has been explained in detail in Chapter 4.</td></tr>
<tr><td>Audit Frequency</td><td>Internal audit should use the audit frequency grid as a guide in the annual planning and scheduling of audits. Audit frequency is an indication of the likely interval to the next audit. Audit frequency will be decided planned based on the risk rating as follows.

<table><tr><th>Risk rating</th><th>Audit Frequency</th></tr><tr><td>Low</td><td>Once in 3 years</td></tr><tr><td>Medium</td><td>Annually</td></tr><tr><td>High</td><td>Monthly/Quarterly/Half Yearly/Annually</td></tr><tr><td>Extremely High</td><td>Monthly/Quarterly/Half Yearly/Annually</td></tr></table>
All functional audits have to be conducted once in 3 years even if they are graded as low risk.

Where the ACB recommends changes to the Audit frequency for selected Units in the Audit Universe, the same will be incorporated in the IA plan.</td></tr>
<tr><td>Annual Audit Planning and Scheduling</td><td>The Annual Audit Plan and Audit Schedule should be prepared based on Risk Assessment performed. Prioritization of the audits in the annual audit planning should be based on processes with high intrinsic risk and probability values. Audit Planning exercise shall ideally be initiated in January every year and completed before the last ACB of the previous financial year.

Any other process or area identified by Statutory Auditor, RBI Auditor or management would be prioritized.

The RBIA Plan should broadly contain the following elements:

• Number of audits to be carried out during the year
• Locations/Processes to be audited during the year
• Tentative Audit Schedule / Timeline for audit
• Risk rating of process / location</td></tr>
</table>

Presentation of Audit Plan to the ACB	The RBIA Plan, post conclusion of the risk assessment shall be discussed with Senior Management and any changes required basis their feedback will be made. The senior management is responsible for ensuring adherence to the internal audit policy guidelines as approved by the Board and development of an effective internal control function that identifies, measures, monitors and reports all risks faced. It shall ensure that appropriate action is taken on the internal audit findings within given timelines and status on closure of audit reports is placed before the ACB/Board The proposed annual audit plan and schedule shall be circulated to the senior management for inputs and submitted to the ACB for approval. Any changes suggested by ACB shall be incorporated in the IA Plan. The monthly progress report of internal audit plan shall be reported to Senior Management.
Resource Budgeting	Senior management is responsible for establishing a comprehensive and independent internal audit function which should promote accountability and transparency. It shall ensure that the RBIA Function is adequately staffed with skilled personnel of right aptitude and attitude who are periodically trained to update their knowledge, skill and competencies. Internal Audit Department shall also do the Resource budgeting parallel to the Annual audit planning. Resource budgeting will consider the following elements: • Complexity and coverage of the unit • Experience and skill sets of the Internal Auditor The overall elements shall be mapped against the available resources to work out Resource plan for the year. The resource plan shall be discussed and approved by HIA. Where skill sets are not available with Internal Audit, the HIA shall consider hiring experts for specialized audits depending on the circumstances.
Preparing Audit Calendar	Audit schedule will be prepared along with assigned resources for each audit.

CHAPTER 3: AUDIT EXECUTION LIFECYCLE	
Conducting an Audit as per approved Audit Plan	Internal Audits should be conducted in accordance with the approved audit plan. The audit process methodology should include the following steps: i. Announcement of the Audit along with Scope of Audit and Tentative Timelines ii. Preparation of Audit Program iii. Opening Meeting and briefing of audit approach iv. Audit Fieldwork –Process walkthrough and data analysis v. Raising Audit issues and discussion with stakeholders vi. Supervisory Review of Audit lifecycle and audit work-papers vii. Issuance of Draft Report viii. Closing Meeting with stakeholders ix. Issuance of Final Audit Report x. Tracking of Action Plan and closure Where multiple auditors are assigned to large / complex audits, the responsibility of ensuring adherence to above process steps lies with the Audit Lead and shall be reviewed by the Audit Manager at each step of the process. All communication with stakeholders/ auditee for above process steps shall be done by the Audit Lead. The other team members, however, can communicate with the auditees for data requests and clarifications for the respective areas of work allocated to them. However, formal audit issues shall be issued from the desk of the Audit Lead. In case there is only one team member assigned to an audit, the concerned auditor shall be designated as Audit Lead.
Announcement of Audit	• Before commencement of an audit, A formal communication (e-mail) shall be sent to each audit unit head containing the following information 1) Audit start and end dates, audit period, audit team 2) Initial data requirement maybe shared along with announcement or follow it . 3) Seeking details of a primary contact (SPOC) from audit unit to facilitate coordination of the audit work • The intimation must be sent well in advance usually 1 week before commencing the audit except in cases where surprise or special audits are to be carried out. • E-mail should be released by the Audit Manager/Supervisor • Announcement shall be mailed to the respective HOD, Functional Heads, respective Leadership team, HIA, Audit team members and Audit Manager. Audit lead and audit team members shall be assigned to the audits in consultation with the HIA. The auditee (Function Head) is required to appoint an audit coordinator (SPOC). Initial request for process documents, manuals etc. shall be made with the audit announcement or proceed it.

Preparation of Audit Program	The Audit team should prepare a formal internal audit program which will include the risk control matrix based on the scope documented. Internal audit program should be so designed as to achieve the objectives of the audit and also provide assurance that the internal audit is carried out in accordance with professional standards and approved audit process methodology. **Test Plan**: The testing plan shall be sufficiently detailed to cover all the key controls in the process. If required, if there are multiple controls against a risk, the test steps for each control can be documented in a separate test sheet. The sample size and sampling methodology, rationale for the sample shall be documented in the audit program. **Work allocation**: Depending on team size, the Audit Lead shall allocate the areas of work from RCM to team members. The work allocation shall be communicated to team members on email on timely basis. However, Audit Lead assumes overall responsibility of audit and ensuring all controls are tested The Audit Program shall be reviewed and approved by the Audit Manager and the DGM.
Opening meeting and briefing of Audit approach	Opening meeting should be conducted on the first day of fieldwork prior to commencement of the audit. The opening meeting should include the audit team along with Group Head of Internal Audit / Audit Manager and Respective HOD/ Functional Head / Stakeholders/ Audit SPOC. Objective of the Opening Meeting is to discuss overview by auditee of major processes, programs and operations, new activities / systems, relevant policies and procedures and other information that will assist the audit team in their fieldwork.
Audit Fieldwork Process walkthrough, data analysis and raising Audit issues	Audit fieldwork shall commence after the opening meeting. The following procedures shall be performed during fieldwork: • Review policies and process level documentation • Interview department personnel, if required • Walkthrough of process and systems • Physical visit to locations etc. • Selection of samples and analysis of documents and transactions • Data analytics within the process or adopt sampling methodology to verify the operating effectiveness of controls • Evaluation of controls in place to mitigate these risks • Raise audit issues in the absence of adequate controls/ deficiencies in existing controls / non-adherence to existing controls. • Audit issues shall be rated as high / medium / low depending on the assessment of risk. Process Improvement Opportunity (PIO) shall be raised as PIO and shall not be graded. . Audit Lead shall ensure that the results of test of design and operating effectiveness of controls are documented. Audit issues shall be raised immediately during the course of fieldwork and shall be mailed to Auditee SPOC, HOD, audit team, HIA. The auditee is required to provide management action points and target dates for completion of the action points. Audit issues shall be reviewed by the Audit Manager before they are released to the Auditee.
Supervisory Review of Audit	The Audit Manager shall conduct review of audit quality and progress with the Audit Lead and team members at each step of the Audit lifecycle and conduct review meetings.

<table>
<tr><td>Closing Meeting and Issuance of Draft & Final Audit Report</td><td>Closing meeting Once all issues are discussed with the relevant process owners and agreed, closing meeting will be conducted with the relevant Functional Head at the level of GM / SVP. Audit Team will issue draft report to the stakeholders. The closing meeting shall include, process owners, audit SPOC , Audit team, Audit Manager and DGM. The stakeholders shall be apprised of the final audit issues and their concurrence obtained along with management action plan and target dates

At the closing meeting, assuming that all audit issues have been satisfactorily responded, the HIA can officially announce the final audit grading of the audit.</td></tr>
<tr><td>Issuance of Final Report</td><td>The internal auditor should ensure that agreement on the audit issues raised should exist between the auditor and auditee prior to issuance of the final audit report. In the event that responses to any particular audit issue(s) are not received at time of final audit report issuance, IA will proceed to issue the report and indicate that responses have not been received from the auditee. This will ensure that the entire audit process is not delayed due to non-receipt of responses from the auditee.The Final Audit report shall be reviewed and released by the HIA to the respective HOD, Functional Head with a copy to the CFO/Whole Time Director. Copy of the IA report shall be shared with HCL IA Group.</td></tr>
<tr><td>Tracking of Action Plan and closure</td><td>The purpose of observation Action Plan tracking is to control the progress by management of the remediation of observations reported by Internal Audit and to assess the adequacy of the remediation measures implemented by management.

Respective Audit Lead shall ensure that audit issues raised in the final report are updated in the observation tracker maintained in the Common IA Drive along with the Corrective Action Plan. Escalations would be marked to the stakeholder’s leadership team on quarterly basis.

<table>
<tr><td>Number of days post closure date of action plan</td><td>30</td><td>60</td><td>90</td></tr>
<tr><td>Escalate the issue to level</td><td>Reporting manager of person responsible. CC to person accountable</td><td>Person accountable</td><td>Reporting manager of person accountable</td></tr>
</table>

Regular follow-up to be carried out on all the open audit observations by the respective Auditors and update the status in the observation tracker.

Observations closed by auditee should be reviewed by Audit Lead within 30- 90 days (of closure) to validate implementation for high, medium and low risk observations. Audit evidences shared by auditee for closure of observations and closure validation report shall be saved in the respective Audit folder. The closure validation comments shall also be updated in the Observation tracker by the respective Audit Lead.</td></tr>
</table>

CHAPTER 4: RISK ASSESSMENT	
Introduction	The Internal Audit function shall perform an independent risk assessment of all the auditable units identified in the Audit Universe for the purpose of formulating a Risk based Internal Audit (RBIA) Plan. Risk assessment is a systematic process for identifying and evaluating events (i.e., possible risks and opportunities) that could affect the achievement of objectives, positively or negatively. Such events can be identified in the external environment (e.g., economic trends, regulatory and landscape) and within an organization's internal environment (e.g., people, process, and infrastructure). Risk Management Function should focus on identification, measurement, monitoring, and management of risks, development of risk policies and procedures, use of risk management models, etc., Internal Audit Function should undertake an independent risk assessment for the purpose of formulating a risk-based audit plan which considers the inherent business risks emanating from an activity / location and the effectiveness of the control systems for monitoring such inherent risk
Risk assessment frequency	The risk assessment in the internal audit department should be used for focusing on the material risk areas and prioritizing the audit work. The risk assessment of all functions and processes would be conducted on an annual basis. The assessment shall be updated to account for changes in business environment, activities and work processes, etc., if necessary. Risk assessment should include assessment of the inherent, control and residual risks. Changes in the Audit Plan necessitated due to re-assessment of risk shall be reviewed by HIA and placed with the ACB for ratification.
Risk Assessment Methodology	**Risk assessment would include the following steps.** • **Inherent risks assessment:** Events identified as potentially impeding the achievement of objectives are deemed to be risks and should be evaluated based on the likelihood of occurrence and the significance of their impact on the objectives. It is important to first evaluate such risks on an inherent basis, that is, without consideration of existing risk responses and control activities. Inherent risks shall be assessed on a scale of 1-3, 1 = Low, 2=Medium, 3= High risk • **Control risk assessment**: The Internal Audit function, in consultation with the business units and support functions, will identify control risk element and define parameters. The Internal Audit function will leverage the Operational Risk Management results /parameters, Internal Financial Controls, past audit history/ regulatory inspection, legal and compliance etc. for identification of control risks parameter for each unit/process. Control risks shall be assessed on a scale of 1-3. 1 = Low, 2=Medium, 3= High control. Obtain key inputs from the Risk and Compliance functions, Leadership Team, Statutory Auditor and the ACB and/or Board • **Residual risk assessment:** Residual risk assessment considers both the risks as previously identified and the related risk response mechanisms and control activities in place to determine the impact and likelihood of their occurrence. In other words, it evaluates the adequacy and effectiveness of the internal checks and balances in place, providing reasonable assurance that the likelihood and impact of an adverse event is brought down to an acceptable level. Residual risk shall be arrived at by subtracting the control risk rating from the Inherent risk rating. Residual risk shall be assessed on a scale of 1-3. .

Risk assessment parameters	Parameters that may be used in assessing the risks are viz. (not exhaustive): • Objective of the unit/processes and associated risks and internal control systems. • Previous internal audits and status of compliance. If the previous internal audit rating of process is Improvement required, the residual risk rating shall be High. If the previous internal audit rating of the process is unsatisfactory, the residual risk rating shall be Extremely High. • changes affecting the function like changes in management / key personnel, business processes, information technology, regulatory / legal environment, • results of regulatory inspections • reports of external auditors • industry trends and other environmental factors • time elapsed since last audit • volume of business and complexity of activities • substantial performance variation from budget • business strategy vis-à-vis the risk appetite and adequacy of control • extent of automation of processes and outsourcing of processes and control activities. • Operational Risk/ Fraud losses The basis of determination of the level (very high/high, medium, low) of inherent risks and controls shall be clearly spelt out in the risk assessment document. The risk assessment parameters shall be reviewed and updated on as & when required.
MIS	For the risk assessment to be accurate, it will be necessary to have proper MIS and data integrity arrangements. The internal audit function should be kept informed of all developments such as introduction of new products, changes in reporting lines, changes in accounting practices / policies, etc. The risk assessment should invariably be undertaken on a yearly basis. The assessment should also be periodically updated to take into account changes in business environment, activities and work processes, etc.
Risk assessment of Information Technology and Information Systems	The detailed procedure of IT & IS risk assessment has been covered in separate chapter.

Rating and Periodicity

Risk Control Matrix:

Inherent Risk	High	High Risk	High Risk	Extremely High Risk
	Medium	Medium	Medium	High Risk
	Low	Low	Medium	High Risk
		Low	Medium	High
		Control Assessment		

CHAPTER 5: INTERNAL AUDIT EVIDENCE & DOCUMENTATION	
Introduction	The internal auditor should, based on his professional judgment, obtain sufficient appropriate evidence to enable him to draw reasonable conclusions and draft his findings, if applicable. Factors affecting professional judgment include the activity under audit, possible errors and their materiality and the risk of occurrence of such errors Documentation means the record of audit procedures performed, including audit planning, relevant audit evidence obtained, and conclusions the audit team has reached (terms such as "Audit Issue Work Papers.
Sufficient, Reliable & Appropriate evidence	The internal auditor is required to gather sufficient, reliable and appropriate evidence during the audit process to substantiate his findings or support his views of the control environment of the unit being audited. The internal auditor's judgment as to what is sufficient and appropriate internal audit evidence is usually influenced by materiality, type of information and risk of misstatement. When internal audit evidence obtained from one source is inconsistent with that obtained from another, or the internal auditor has doubts over the reliability of information to be used as internal audit evidence, the internal auditor shall determine what modifications to, or additional audit procedures are necessary to resolve the same.
Period of Retention and Storage of audit evidence and other documents	Period of Retention: All work papers used during audit are to be saved centrally in a dedicated shared folder created for Internal Audit function. The record retention requirements are detailed in **Annexure 1**
Retrieval of Documents	HIA to manage the access of shared folders thereby managing the retrieval of documents.
Document Destruction	1. Destruction of documents shall be based on the Life of the document as specified in Annexure 1. 2. A complete listing of records to be destroyed shall be signed off by the HIA.

Annexure 1

Name of the Document	Period	Type of Record
Audit Policy and Manual	Permanent	Soft copy
Yearly Audit Plan	7 Years	Soft Copy
File Review documents and reports	7 years	Soft Copy
Supervisory review documents	7 years	Soft Copy
Yearly Risk Assessment Corporate audit	7 Years	Soft Copy
Audit Committee presentation	7 years	Soft Copy
Audit Report for functions and branches	Permanent	Soft Copy
Audit file	7 Years	Soft Copy
Observation Tracker	Permanent	Soft Copy

CHAPTER 6: REPORTING	
Introduction	The Purpose of this chapter is to establish standards on the form and content of the internal auditor's report issued because of an internal audit performed by them. • The internal audit report should contain a clear written expression of significant observations noted during the audit and managements' responses. • The internal audit report should also state the auditor's opinion on the unit's current state of control. • Any repeat of past audit issues raised must also be highlighted in the internal audit report. This will be taken into consideration when determining the final audit grade.
Elements of the Internal Audit Report	The internal auditor's report should include the following basic elements: **i.** **Executive Summary**: The Executive Summary should provide opinion of the state of internal control, major developments in the recent past that has contributed to the improvement or deterioration in the control environment as well as plans to address any control gaps. Key issues/control lapses or weaknesses in systems and processes identified during the audit should also be highlighted in the executive summary. The Executive Summary shall be part of the email communicating the Final Audit report to the auditees. **ii.** **Scope of Work:** The internal audit function should broadly assess and contribute to the overall improvement of the organization's governance, risk management, and control processes using a systematic and disciplined approach. The internal audit report should provide a reference to scope document which mentions the period of coverage for the audit, which would generally be upto 12-month period prior to the audit date. It should also give a background to the audit area, highlight the audit objectives and the audit fieldwork date and time. **iii.** **Date**: The date of an internal auditor's report is the date on which the internal auditor signs / issues the report expressing his comments and observations. **iv.** **Title of the Report**: The internal audit report should have an appropriate title of the audit (for process audits) or name of the business unit being audited. **v.** **Addressee:** The internal audit report should be appropriately addressed to the Head of the function to be audited/reviewed, Head of functions supporting the unit to be audited as well as senior management responsible for the function to be audited. **vi.** **Report Distribution List:** Recipients of the report should be mentioned in this section, **vii.** **Overview of Key Observations:** The report should contain a summary of observations with issue rating classified as High, Medium or Low and root cause classified as design deficiency, operating ineffectiveness or system deficiency. **viii.** **Observations**: The report should contain observations with rating classified as High, Medium or low based on the internal auditor's assessment of risk. **ix.** **Management Action Plan**: Each Audit issue should contain the management's response to the audit issues, action plan to address the same along with target resolution date and Responsible person. **x.** **Audit Team:** The audit report should specify the audit team who has completed the audit. **xi.** **Approval:** The Audit Report should be approved by the Group Internal Audit Head. **xii.** **Restriction on Usage and Report Circulation:** Document classification shall be confidential, and circulation of the report shall be limited to the recipients mentioned in the report. **xiii.** The internal auditor should exercise due professional care to ensure that the internal audit report, inter alia, is Clear, Factual, Concise, Unambiguous, and Complies with generally accepted audit procedures

CHAPTER 7: SAMPLING

Introduction

The purpose of this chapter is to provide guidance on the use of audit sampling in internal audit engagements and evaluation of the sample results. This chapter applies equally to both statistical and non-statistical sampling methods. Either method, when properly applied, can provide sufficient appropriate audit evidence.

Definition

i. "Audit sampling" means application of audit procedures to less than 100% of the items within an account balance or class of transactions to enable the internal auditor to obtain and evaluate audit evidence about some characteristics of the items selected to form a conclusion concerning the population.
Exception to the definition: Certain testing procedures, however, do not come within the definition of sampling. Tests performed on 100% of the items within a population do not involve sampling. Likewise, applying internal audit procedures to all items within a population which have a particular characteristic (for example, all items over a certain amount) does not qualify as audit sampling.

ii. "Population" means the entire set of data from which the sample is selected and about which the internal auditor wishes to draw conclusions. A population may be divided into various strata, or subpopulations, with each stratum being examined separately.

iii. "Statistical sampling" means any approach to sampling procedure which has the following characteristics:
   a. Random selection of a sample; and
   b. Use of theory of probability to evaluate sample results, including measurement of sampling risk.

Design of the Audit Sample

When designing an audit sample, the internal auditor should consider the specific audit objectives, the population from which the internal auditor wishes to sample, and the sample size and suitable sampling technique mentioned below:

1. Random sampling
2. Systematic sampling/ Interval sampling
3. Monetary unit sampling
4. Haphazard sampling
5. Block sampling

Sample Size

Sample Size: 30 items or 10%, whichever is lower. If there are 1 or 2 gaps/exceptions identified, IA team should extend sample size by another 10-20 items to ascertain whether control failure is systemic. For automated controls, the minimum sample size is one, if the underlying general IT controls are deemed effective.

Frequency of Control Activity and Sample size
Minimum sample size may be determined based on the frequency of control activity as follows:

Frequency of Control Activity	Minimum Sample Size
Annual	1
Half-Yearly	1
Quarterly	2
Monthly	2
Weekly	5

Evaluation of Sample Results	Having carried out appropriate audit procedures on each sample item, the internal auditor should: i. analyze the nature and cause of any errors detected in the sample. ii. project the errors found in the sample to the population. iii. reassess the sampling risk; and consider their possible effect on the internal audit objective and on other areas of the internal audit engagement. The internal auditor should evaluate the sample results to determine whether the assessment of the relevant characteristics of the population is confirmed or whether it needs to be revised. If the evaluation of sample results indicates that the assessment of the relevant characteristics of the population needs to be revised, the internal auditor may: i. Request management to investigate the identified errors and the potential for any further errors, and to make necessary adjustments, in cases where management prescribes the sample size; and / or ii. Modify the nature, timing and extent of internal audit procedures. In case of tests of controls, the internal auditor might extend the sample size, test an alternative control or modify related substantive procedures; and / or iii. Consider the effect on the Internal Audit Report.

CHAPTER 8: ANALYTICAL PROCDEDURE	
Introduction	The purpose of this chapter is to establish standards on the application of analytical procedures during an internal audit. "Analytical procedures" means the analysis of significant ratios and trends, including the resulting investigation of fluctuations and relationships in both financial and non-financial data that are inconsistent with other relevant information or which deviate significantly from predicted amounts.
Nature and Purpose of Analytical Procedures	Analytical procedures include the consideration of comparisons of the entity's financial and non-financial information with, for example: i. Comparable information for prior periods. ii. Anticipated results of the entity, such as budgets or forecasts or expectations of the internal auditor. iii. Predictive estimates prepared by the internal auditor, such as an estimation of depreciation charge for the year, and gross margin percentages. iv. Similar industry information, such as a comparison of the entity's ratio of sales to trade debtors with industry averages, or with other entities of comparable size in the same industry. iv. Comparison between financial information and relevant non-financial information, such as payroll costs to number of employees or total production costs to quantity produced. Analytical procedures may also include analysis of population data of the area under review wherever available for compliance with relevant policies / procedures, identify trends / discrepancies / potential control weaknesses.
Extent and Use of Analytical Procedures	Analytical procedures are used for the following purposes: i. assist the internal auditor as risk assessment procedures to obtain initial understanding of the entity and its environment and thereafter in planning the nature, timing and extent of other internal audit procedures. ii. as substantive procedures when their use can be more effective or efficient than tests of details in reducing detection risk for specific financial statement assertions. iii. as an overall review of the systems and processes in the final review stage of the internal audit; and iv. To evaluate the efficiency of various business/ management systems.
Investigating unusual items or trends	When analytical procedures identify significant fluctuations or relationships that are inconsistent with other relevant information or that deviate from predicted amounts, the internal auditor should investigate and obtain adequate explanations and appropriate corroborative evidence. Results or relationships that are not sufficiently explained or correlated should be communicated to the appropriate levels of management. The internal auditor may recommend appropriate courses of action, depending on the circumstances.

CHAPTER 9: COMMUNICATION WITH MANAGEMENT	
Introduction	This Chapter provides a framework for the internal auditor's communication with management and identifies some specific matters to be communicated with the management.
Matters to be communicated	**Matters to be communicated with Management:** **Planned Scope and Timing of the Internal Audit:** Communication regarding the planned scope and timing of the internal audit may assist the management to correctly understand the objectives of the internal auditor's work. • to discuss issues of risk and materiality with the internal auditor; and • to identify any areas in which they may request the internal auditor to undertake additional procedures When communicating to management about planned scope and timing of the internal audit, it should be ensured that it does not reduce the effectiveness of internal audit. **Significant Findings from the internal audit-** During the fieldwork phase, the internal auditor shall discuss findings and potential recommendations with the auditee for comments and feedback **Draft Report -** Draft report of all observations that have been issued and discussed with the auditee should be consolidated along with Management responses where received should be issued to the HOD on completion of fieldwork and testing. **Closing Meeting –** The internal auditor should discuss with the Management of the audited entity on the findings, observations and audit issues raised in the draft report. The Management of the unit should discuss the audit issues with the internal auditor and provide appropriate responses to address the control gaps identified during the audit. **Final Report** – HIA is responsible for approving all internal audit reports and this should be communicated to concerned stakeholders &~~,~~ Higher Leadership team. **Report to ACB / Leadership Team:** Internal Audit function is responsible for presenting high and moderate observations noted during the audits to the ACB. In line with the IA charter, the HIA should apprise the ACB on the observations noted, along with the action to be considered and the timeline for closure of the audit finding. All the pending high and medium risk findings and persisting irregularities shall be reported to the ACB to highlight key areas in which risk mitigation has not been undertaken despite risk identification. A consolidated position of major risks faced by the organization shall be presented at least annually to the ACB/Board, based on inputs from all forms of audit. **Content of the Report to the ACB shall be as below**: • Executive Summary. It summarizes the contents of the report and addresses any areas of interest including staff activity, special projects, or key concerns/roadblocks etc. • Summarizes the audits conducted for the year/period. The major audit objectives are described by audit type. • Summarizes the results of all the key audit recommendations and status of follow-up points in result of audits performed during year/half year. In addition, statistics that illustrate the total number of recommendations and status of follow-up and the corresponding results are provided. • A summary of the audits planned for the next fiscal year categorized by major transaction cycle/business **Limitation of Scope:** When there is a limitation on the scope of the internal auditor's work, the internal

Documentation	Where matters are communicated orally, the internal auditor shall document the communication on mail with the relevant stakeholder and retain the email as part of audit documentation. Where matters have been communicated in writing, the auditor shall retain a copy of the communication as part of the internal audit documentation.
Communication with ACB	The following will be points of communication with ACB on quarterly: • Status of Follow-up items arising from ACB • Annual review of Internal Audit Policy • Status update on audit plan, • High / medium risk observations raised since last ACB and status of same • Status of high/medium risk observations raised and open till date • Annual / Half yearly update on Risk assessment

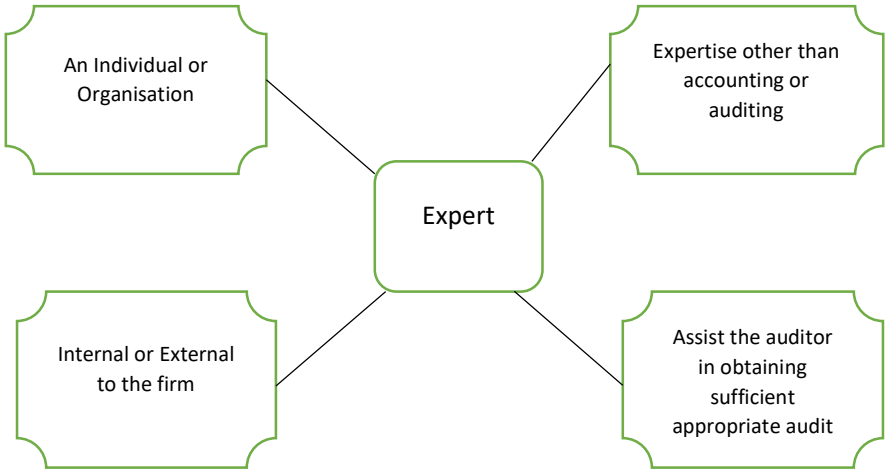
CHAPTER 10: CONSIDERATION OF FRAUD IN INTERNAL AUDIT	
Introduction	Fraud is defined as an intentional act by one or more individuals among management, those charged with governance, or third parties, involving the use of deception to obtain unjust or illegal advantage. The primary responsibility for prevention and detection of frauds rests with management and those charged with governance. They achieve this by designing, establishing and ensuring continuous operation of an effective system of internal controls.
Reasonable Care	Internal Auditor must exercise reasonable care and professional skepticism while carrying out internal audit to evaluate possible risk of frauds.
Responsibilities of The Internal Auditor	The primary responsibility for prevention and detection of frauds is that of the management. The internal auditor should, however, help the management fulfill its responsibilities relating to fraud prevention and detection. The internal auditor can adopt the following approach: **i. Control Environment** The internal auditor should obtain an understanding of the various aspects of the control environment and evaluate the same as to the operating effectiveness. **ii. Risk Assessment** In the context of prevention of frauds, the internal auditor should specifically evaluate the policies and procedures established by the management to identify and assess the risk of frauds, including the possibility of fraudulent financial reporting and misappropriation of assets. **iii. Information System and Communication** The internal auditor should assess the operating effectiveness of the policies and procedures established by the management to identify, capture and communicate relevant information to the concerned persons in the entity to enable them to make timely and effective decisions and discharge their responsibilities efficiently. **iv. Control Activities** The internal auditor should assess whether the controls implemented by the management, are in fact working effectively and whether they are effective in prevention or timely detection and correction of the frauds or breach of internal controls. **v. Monitoring** The internal auditor should evaluate the mechanism in place for supervision and assessment of the internal controls to identify instances of any actual or possible breaches therein and to take corrective action on a timely basis. **vi. Communication of Fraud** Internal Auditor shall immediately bring, actual or suspected fraud or any other misappropriation of assets, to the attention of the FCU for further investigation. This should also be summarized in ACB deck. **vii. Documentation** The internal auditor should document fraud risk factors identified as being present during the internal

CHAPTER 11: USING WORK OF AN EXPERT

Introduction

"Expert "means a person or firm possessing special skills, knowledge and experience in a particular field other than auditing.

WHO IS AN EXPERT?



The Need of an Expert

During the audit plan stage, it is assessed to obtain assistance of an expert to perform an audit/audits the same to be put off for approval of Whole Time Director / ACB.

The scope of work of expert shall be defined in written instructions. Such instructions to the expert may cover the following matters in a written agreement with the expert:

a. The objectives and scope of the expert's work.
b. A general outline as to the specific matters the internal audit expects the expert's report to cover.
c. The intended use by internal audit of the expert's work, including the possible communication to third parties of the expert's identity and extent of involvement.
d. The extent of the expert's access to appropriate records and files.
e. Clarification of the expert's relationship with the auditee, if any
f. Confidentiality of the auditee's information.

Assessing the Work of an Expert	The Internal Audit Department should assess the work of the expert as follows: a. Assessing the work in consideration with source data used, assumptions and methods used and their consistency with prior periods, reason for any changes in assumptions and methods. b. Results of the expert's work in the light of the internal audits overall knowledge of the business and the results of other audit procedures. c. Making enquiries regarding any procedures undertaken by the expert to establish whether the source data is sufficient, relevant and reliable. d. Reviewing or testing the data used by the expert. i. If the internal audit is not satisfied, that the work of an expert provides sufficient appropriate audit evidence and there is no satisfactory alternative source of such evidence, the internal audit would consider the implications for the report and document the same. ii. In exceptional cases where the work of an expert does not support the related representations in the overall systems, procedures and controls of the auditee, the internal audit should attempt to resolve the inconsistency by discussions with the auditee and the expert by applying additional procedures. The internal audit may also engage another expert in resolving the inconsistency.

CHAPTER 12: INFORMATION SYSYTEM AUDIT	
Introduction	The purpose of this chapter is to establish standards and provide guidelines on information systems audit in Vama Sundari Investments (Delhi) Pvt. Ltd.
Skills and Competence	IS Audit may be conducted by an internal team of the Vama Sundari Inv Delhi Pvt Ltd.. In case of inadequate internal skills, Vama Sundari Investments (Delhi) may appoint an outside agency having enough expertise in the area of IT/IS audit for the purpose subject to compliance with RBI regulations. There should be a right mix of skills and understanding of legal and regulatory requirements so as to assess the efficacy of the framework vis-à-vis these standards. IS Auditors should act independently of Vama Sundari Inv Delhi Pvt Ltd.'s Management both in attitude and appearance. In case of engagement of external professional service providers, independence and accountability issues may be properly addressed. IS Auditors should preferably be a CISA certified professional.
Scope	IS Audit should cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up.The internal auditor should review the robustness of the IT environment and consider any weakness or deficiency in the design and operation of any IT control within the company at least once in a year, preferably prior to Statutory audit, by reviewing: a. System Audit reports of Vama Sundari Inv Delhi Pvt Ltd., conducted by independent Information System auditors; b. Reports of system breaches, unsuccessful login attempts, passwords compromised and other exception reports; c. Reports of network failures, virus attacks and threats to perimeter security, if any; d. General controls like segregation of duties, physical access records, logical access controls; e. Application controls like Data input / output validations, Data processing, Storage, retrieval and communication, Backup and recovery, Access control, Operating System Controls, Database Controls. f. Effectiveness of business continuity planning, crisis management and disaster recovery procedures. g. IT continuity framework plan and testing; h. Change management process and Testing, approval and monitoring of changes. i. Release management process and testing, approval and monitoring of releases j. Vendor Risk management process. k. RBI Daksh portal access quarterly review for UAM, operations and security controls l. License management process and Licensed software implementation and tracking m. Network Security management like Perimeter security, Segregation of environments, LAN, WAN, VPN security. n. Physical Security and Environmental Controls of the server rooms (communication). o. Security Management of Information Security policies and standards, User Access Management process (AD), Administrative access management, Data leakage prevention, Data backup & retention. p. Compliance to applicable Legal, Statutory and Regulatory requirements and IT policies. q. Application control / network /server/ cloud If the internal auditor is not able to rely on the effectiveness of the IT environment as a result of the review, he may perform such substantive testing or test of IT controls, as deemed fit in the circumstances. The internal auditor should apply his professional judgment and skill in reviewing the IT environment and assessing the interfaces of such IT infrastructure with other business processes.
Periodicity	The IS audit must be conducted at least once in a year. IS Audit should be undertaken preferably prior to the statutory audit so that IS audit reports are available to the statutory auditors well in time for examination and for incorporating comments, if any, in the audit reports.

Observation tracker	Vama Sundari Inv Delhi Pvt Ltd.'s management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IS Audit. Responsibilities for compliance/sustenance of compliance, reporting lines, timelines for submission of compliance, authority for accepting compliance should be clearly delineated in the framework.

Risk Assessment of IT & IS

The scope of the IS audit shall be decided based on the detailed Annual IT & IS Risk assessment carried out as follows:

1. Assessment of Inherent and Control risk

A. At Process Level:

- Each process and sub-process of an auditable unit shall be assessed basis its Inherent risk and control risk.

- Inherent risks of each process of an auditable unit will be evaluated based on the following criteria:

  - Regulatory implications: Primarily RBI master directions, IT Act
  - Information security risk considerations: based on reference to ISO27K / NIST framework and whether there is a risk sensitive information being compromised associated with the auditable unit
  - Relevance to financial reporting: Domains mapped in ITGC RCM

- Control risk for each process shall be evaluated based on the following factors:
  - Past audit observations: including IA / RBI Inspection observations.
  - Number of preventive controls: The preventive controls have been identified in the ITGC Risk registers for technology which are maintained separately for applications. The segregation between preventive / detective controls was performed based on the nature of the control. The controls in review / reconciliation have been categorized as detective. The extent of preventive controls was classified as Significant, medium and minor based on the below criteria.

Classification	***% of preventive controls***	
	Low band	***Upper band***
Minor	***0***	***25***
Medium	***26***	***60***
Significant	***61***	***100***

  - The above percentages were derived based on the controls for each of the following areas:
    - User Management (Categories clubbed in the RCM: SOD, System Configuration for authentication, User Access De-Provisioning, User Access Modification, User Access Provisioning, User Access Review).
    - Change Management
    - Back up
    - Batch jobs

B. At Application Level:

- Each application and underlying infrastructure shall be classified based on whether they:
  - Process Financial transactions
  - Internet facing
  - Business Impact in case of application in accessible.
  - Interfaces with other applications
  - Automated controls dependent on the application
  - Relevant to regulatory compliances / reporting

Risk	***Number of application rating criteria***
High	***More than 5 factors***
Medium	***4 factors***
Low	***Up to 3 factors***

Final rating for inherent and control risk rating for each auditable area

Risk Definition for Inherent Risk/ Control Risk		
Risk	***Inherent risk***	***Control risk***
High	all the inherent risk criteria	Past audit observations and / or < 25% preventive controls
Medium	2 of 3 inherent risk	Past audit observations and / or 25-60% preventive controls
Low	1 out of 3 inherent risk	No audit observations and / or > 60% preventive controls.

The criteria for final classification of the Auditable unit		
IR CR combination	**Final risk rating**	**Frequency**
HH	Extremely high risk	Once in half a year
HM or MH	High risk	Once in a year
HL or LH	High risk	Once in a year
MM	Medium risk	Once in a year
ML or LM	Medium risk	Once in two years
LL	Low risk	Once in three years

Risk Control Matrix:

Inherent Risk	High	High Risk	High Risk	Extremely High Risk
	Medium	Medium	Medium	High Risk
	Low	Low	Medium	High Risk
		Low	Medium	High
		Control Assessment		

IS Audit Report

IS audit report shall also be placed to the ACB by the Head of Internal Audit.

CHAPTER 13: SUPERVISORY REVIEW	
Introduction	Supervisory review is a process instituted in Internal Audit function to ensure quality of audit, adherence to audit policy and procedures and maintenance of adequate audit documentation.
Scope	The scope of supervisory review covers the entire lifecycle beginning from audit announcement, audit planning, scoping, fieldwork, audit documentation and workpapers, evidencing performance of audit procedures, closing meeting and issuance of final audit report and tracking and closure of audit observations.
Responsibility	• Internal Audit Managers are responsible for performing supervisory review. • Respective Internal Audit Managers / Audit Leads shall review the quality of work performed by their audit executives on an ongoing basis.
Elements of Supervisory Review	Few critical parameters of supervisory review are as follows. Audit Manager shall: • Ensure that the audit lifecycle process steps are followed. • Review the scope of audit to ensure that key inherent risks are covered, and scope is sufficient to mee audit objectives, audit staff is at arm's length from the unit that is being audited, changes in scope o work, if any, is approved by HIA. • The risk ratings are appropriate. • Review the progress and quality of audit work at each step of the audit lifecycle on an ongoing basis. • Review the quality of sample tested. • Review the adequacy of sampling and whether the data is obtained from proper source and saved i the audit documentation; review the clarification obtained for auditees where audit evidence are no appropriate or not provided by the audit team; review the justifications when an issue has been droppe and appropriate evidence is provided and retained as part of audit documentation; wherever the sampl test results of testing shows non-adherence as designed; • Ensure audit issues are raised based on information and not on assumption, root cause is provided i the audit issue and recommendation is provided to prevent recurrence of the issue. • Audit related documents, work papers are saved in the respective audit folder.

CHAPTER 14: BASIC PRINCIPLES OF GOVERNING AN AUDIT	
Fundamental Principles of Audit	The Code of Ethics sets out the fundamental ethical principles that all professional Auditors are required to observe, including: i. Integrity ii. Independence iii. Objectivity iv. Confidentiality v. Due Professional Care, skills and competence vi. Professional Skepticism vii. Documentation viii. Work Performed by others ix. Planning x. Evidence xi. Internal Control and Risk Management Systems xii. Reporting

Integrity	• The Internal Auditor shall be honest, truthful, ethical, fair, observe the law and be a person of high integrity and shall perform their work with honesty, diligence, and responsibility. • The Internal Auditor shall not knowingly be a party to any illegal activity or engage in acts that are discreditable to the profession of internal auditing or to the organization. • The Internal Auditor shall avoid all conflicts of interest and shall not seek to derive any undue personal benefit or advantage from his/her position. • The internal audit function should assess and make appropriate recommendations to improve the governance processes on business decision making, risk management and control; promote appropriate ethics and values within the organization; and ensure effective performance management and staff accountability, etc
Authority, Stature Independence and Resources	The internal audit function must have sufficient authority, stature, independence and resources thereby enabling internal auditors to carry out their assignments properly. The Head of Internal Audit (HIA) shall be a senior executive with the ability to exercise independent judgement. The HIA and the internal audit functionaries shall have the authority to communicate with any staff member and get access to all records that are necessary to carry out the entrusted responsibilities. The internal auditor should immediately bring any actual or apparent conflict of interest to attention of an appropriate level of management so that necessary corrective action may be taken. • The auditors' thinking and judgment will not be influenced by any other considerations in discharge of professional duties. • Auditor will not be influenced by the auditee or anybody in terms of the methodology adopted in conducting an audit, the extent of his verification and the reporting requirements.
Objectivity	The objectivity of an auditor may be classified into two categories i.e., expression of opinion on the state of control within a unit, the design and control effectiveness of the unit taking into consideration major developments in the recent past as well as planned changes soon.
Confidentiality	• The Internal Auditor shall, always, maintain utmost confidentiality of all information acquired during the course of the audit work • Information shall be disclosed to parties outside Internal Audit function only on 'Need to know' basis and with prior approval of HIA • Internal audit reports shall be addressed and distributed only to the specified internal auditees and
Due Professional Care, Skills and Competence	• Due professional care" signifies that the Internal Auditor exercises reasonable care in carrying out the work, to ensure the achievement of planned objectives. However, "Due Professional Care", neither implies nor guarantees infallibility, nor does it require the Internal Auditor to go beyond the established scope of the engagement. • The Internal Auditor shall pay due care in establishing the scope to prevent omission of important aspects, recognizing risks and materiality of the audit areas. • The Internal Auditor shall either have or obtain knowledge, skills and other competencies including technical knowledge, for the purpose of discharging his/her responsibilities. • The Internal Auditor also has a continuing responsibility to maintain professional knowledge and skills based on latest developments in the profession, the economy, the relevant industry, and legislation. • Requisite professional competence, knowledge and experience of each internal auditor is essential for the effectiveness of internal audit function. The areas of knowledge and experience may include banking/financial entity's operations, accounting, information technology, data analytics, forensic investigation, among others. The collective skill levels should be adequate to audit all areas of the Company.

Professional Skepticism	The internal auditors shall apply professional skepticism throughout the planning and performance of the audit. Internal auditor shall - • not accept the evidence gathered at face value • critically assess the evidence without being overly suspicious or cynical • corroborate management explanations or representations concerning material matters
Documentation	The Internal Auditor would document matters which are important in providing evidence that the audit was carried out in accordance with the Standards on Internal Audit and support their findings or the report submitted.
Work Performed by Others	Team Leader should carefully direct, supervise and review the work delegated to the team members, including co-sourced partner. Similarly, auditor may need to use the work performed by other auditors or experts. Though the internal auditor can rely on work performed by others, they should exercise adequate skill and care in evaluating, analyzing and using the results of the work performed by others.
Planning	The internal auditor should plan their work to enable them to conduct an effective internal audit in a timely and effective manner, ensuring that appropriate attention is devoted to significant areas of audit, identification of potential problems and appropriate utilization of skills and time of the staff. A plan once prepared should be continuously reviewed by the internal auditor to identify any modifications to the plan required to bring the same in line with the changes, if any, to the audit universe.
Evidence	The Internal Auditor would, based on their professional judgment, obtain sufficient appropriate evidence to enable them to draw reasonable conclusions or form their opinion on a particular area of control or the lack of, discuss it with the auditee at length before raising an audit issue.
Internal Control and Risk Management Systems	While the management is responsible for establishment and maintenance of appropriate internal control and risk management systems, the role of the internal auditor should be "to provide an independent assessment of the adequacy of the internal control and risk management systems to mitigate the inherent risks of the unit audited".
Reporting	The internal auditor should carefully review and assess the conclusions drawn from the audit evidence obtained, as the basis for their findings contained in his report. However, in case the auditor comes across any actual or suspected fraud or any other misappropriation of assets, he should bring the same immediately to attention of the management.
Reporting line for HIA	The HIA shall directly report to either the ACB/Board or to the Whole Time Director (WTD). Should the Board of Directors decide to allow a WTD to be the 'Reporting authority', then the 'Reviewing authority' shall be the ACB/Board and the 'Accepting authority' shall be the Board in matters of performance appraisal of the HIA.
Code of Conduct for Internal Auditors	The internal auditor needs to be trained on the code of conduct annually.
Quality Assurance and Improvement Program	The ACB/Board should formulate and maintain a quality assurance and improvement program that covers all aspects of the internal audit function. The quality assurance program may include assessment of the internal audit function at least once in a year for adherence to the internal audit policy, objectives and expected outcomes. Further, ACB/Board shall promote the use of new audit tools/ new technologies for reducing the extent of manual monitoring / transaction testing / compliance monitoring, etc.